#18 cw
1-30 cw

UNITED STATES PATENT & TRADEMARK OFFICE

Application No.	:	09/521,636
Title	:	SECURE TRANSACTION PROCESSING SYSTEM AND METHOD
Applicant	:	Andrew Casper
Filed	:	March 8, 2000
TC/AU	:	3628
Examiner	:	Frantzy Poinvil
Docket No.	:	105026/0002

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

DECLARATION OF ANDREW CASPER

UNDER 37 C.F.R. SECTION 1.132

1/31/04

Certificate of Mailing (37 C.F.R. 1.8)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450, on January 12, 2004.

Typed or printed name of person signing this certificate:

Richard Eskew

Signature

1. I am the sole inventor of the above-referenced patent application for a Secure Transaction Processing System filed on March 8, 2000 and claiming priority to Provisional Patent Application Serial No. 60/157,774 filed on October 5, 1999.

2. I am making this Declaration in support of a concurrently filed Amendment in response to the outstanding Office Action of August 14, 2003 in which the Examiner rejected all of the claims pending in the present application. I have reviewed the rejections made by the Examiner, including the cited references and the Examiner's rationales in making the rejections.

3. This Declaration and the attached exhibits describe and evidence the non-obviousness of the claimed invention, and, in particular, set forth the long-felt, but unresolved, need in the relevant on-line purchasing industry for a system that adequately counteracts theft and use of sensitive financial information to make fraudulent purchases over the Internet and other networks. Furthermore, this Declaration and the attached exhibits show the nexus of the claimed invention to solving this long-felt, but unresolved, need in the on-line purchasing industry.

CREDIT CARD/DEBIT CARD FRAUD IS A LONG STANDING PROBLEM

4. Credit card or debit card fraud, e.g., the theft and use of credit card and debit card numbers to make fraudulent purchases, has been an industry wide problem for both merchants and consumer for many years. For instance, on Visa's web site, a summary of the history of Visa U.S.A. notes that, in 1984, "the rapid growth of the payment card industry in mid-80s leads to a rise in credit card fraud and counterfeiting." See Exhibit 1, p. 2.

5. In an August 1997 publication of the Federal Trade Commission ("FTC"), Bureau of the Consumer Protection, Office of Consumer and Business Education, the FTC outlined

various facts to help consumers guard against credit card fraud. See Exhibit 2. In the publication, the FTC noted that credit and charge card fraud cost cardholders and issuers hundreds of millions of dollars each year. See id. at p. 2.

6. Because merchants often suffer the most from credit/debit card fraud in the form of "charge-backs", merchants have banded together to form several consortiums to combat credit/debit card fraud. Once such group that I am aware of is Merchant 911, which can be found at http://www.merchant911.org.

E-COMMERCE COMPLICATES CREDIT/DEBIT CARD FRAUD PROBLEM

7. The emergence of the Internet and online purchasing has only exacerbated the problem of credit/debit card fraud, because the purchaser is not present at the point of sale and the merchant must rely solely on the credit/debit card number transmitted to its system. See Exhibit 3 ("It's much easier to commit fraud online because you're not authenticating the buyer."). As such, credit/debit card fraudsters can use acquired numbers with virtual impunity.

8. To date, despite attempts from credit card companies, banks, merchants, and even consumers, credit card fraud has grown in comparison to the rate of growth of e-commerce. See Exhibit 4, p. 1 ("While e-commerce has grown by nearly 74 percent in the past year, the amount of fraudulent transactions has grown even faster, jumping 114 percent."). Moreover, credit card fraud online accounts for 6.2 percent of all transactions, while such fraud in the normal "brick-and-mortar" world accounts for only about 1 percent. See Exhibit 5, p. 2.

9. Part of the problem with online purchasing using a credit card is that the transmission of credits cards over the Internet to merchants is very susceptible to credit card number theft either at the source (i.e., from the consumer's personal computer), during transmission over the Internet, or from the Merchant who may or may not be trustworthy. By way of example, several large web sites have been hacked and credit cards numbers and other

personal information stolen. See Exhibit 6, p. 2-3. Even the U.S. Department of The Navy has been hacked and had the credit card numbers stolen. See Exhibit 7.

10. In a more recent FTC publication from March 2003, the FTC issued a notice directed specifically at the problem of online credit and debit card fraud as it pertained to the use of electronic payments over the Internet. See Exhibit 8. The FTC recognized that using present systems fraud on the Internet could not be controlled. See id. at p. 3.

11. In a September 2003 FTC report on identity theft, which includes credit/debit card fraud, a survey indicated that it sometimes takes weeks, if not months, for consumers to detect fraud. See Exhibit 9, p. 8. In the case of credit card fraud, according to the survey, it took 61% of consumers longer than one week to recognize the fraud. Id. Of those 61% of consumers, 33% of consumers did not recognize the fraud until after at least one month had passed. Id.

12. Another article from U.S. News.com again recognized the problem of credit card fraud over the Internet. See Exhibit 10. In a statement from Susan Grant, Director of the National Fraud Information Center in Washington, the problem of credit fraud on the internet comes into focus: "no matter how somebody might get a hold of consumer's financial information, the ability to use it on the Internet is huge." Id. at p. 2.

13. Thus, the ability for fraudsters to acquire credits cards used freely on the Internet is one of the main problems plaguing e-commerce. In addition, credit card fraudsters are aided by the fact that current online purchasing systems permit the shipment of goods to any desired location. This creates an enormous loophole in many systems designed to prevent such fraud.

14. The foregoing makes clear that the problem of credit card and debit card fraud has existed for a long period of time and is as of yet, despite many attempts, unresolved. Moreover, the ability of fraudsters to easily obtain credit card numbers freely used for online purchases and then have fraudulent purchases delivered to the location of the fraudster's choice has cost both consumers and merchants millions of dollars each year, and have stunted the growth of Internet

e-commerce as discussed below. See Exhibit 11, p. 2 (Ex. 11 also lists many other articles showing the need for a solution to the problem of online credit/debit card fraud).

ONLINE CREDIT/DEBIT CARD FRAUD HAS HINDERED THE EXPANSION OF E-COMMERCE.

15. In a June 21, 2001 survey by Jupiter Media Metrics, consumers said that they believed their credit card was 12 times more likely to be defrauded on-line than off-line, even though actual data suggested that the occurrence of on-line fraud was just 3 or 4 times that of off-line fraud. See Exhibit 12. Moreover, most internet consumers desire an alternative to having to use their credit card to make online purchases, thus highlighting the need for a solution such as my invention. See Exhibit 13.

16. Despite some recent successes, I believe that online purchasing is being hampered by both the perception and realities of credit/debit card fraud.

17. These trends have not gone unnoticed by major banks and credit card companies, and such companies have taken measures to combat or reduce the risks associated with on-line purchasing. For example, Visa launched its "Next Card" program in 2001 to help consumers protect against someone stealing their personal data. See Exhibit 14. This attempted solution, like many other Internet solutions, focused on encryption techniques for preventing the theft of credit card numbers as they were transmitted over the Internet. Ultimately, however, even Visa recognized that "it is impossible to guarantee that an Internet thief will never get your Next Card Visa number". See id. at p. 3. Visa, like other banks and credit card companies, still did not provide a system that would provide disincentives to using stolen credit card numbers. Thus, the only way for Visa to truly provide a solution to the credit card fraud problem was to guarantee that it would cover the full cost of any fraud against the consumer's account that might arise from fraudulent usage of the next card Visa over the Internet. See id. The Visa solution, therefore, was a downstream and ultimately unsatisfactory solution to the problem for merchants who oftentimes get stuck paying for fraudulent purchases.

18. Visa later introduced a new system referred to as the "Verified by Visa" system. This system simply links a password to a credit card number. The user is still required to transmit both their credit card number and password over the Internet to potentially untrustworthy merchants. See Exhibit 15.

TWO MAIN PROBLEMS TO BE SOLVED

19. The foregoing studies and news articles indicate two distinct, but related, problems with current online purchasing systems. First, because most present systems still require entry of the actual credit/debit card number into a web site form, the number is subject to being stolen by a hacker either from the consumer or the merchant's database. Thus, there is a need for a system that permits online purchases to be made without use of the actual credit/debit card number being entered and transmitted via the Internet to a merchant for authorization.

20. Second, once a credit/debit card number or other code used to make online purchases is stolen, there are no mechanisms currently in place to reduce the ability of the fraudster to make successful fraudulent purchases with the stolen numbers or codes. This is because present systems permit the consumer to change the shipping address to any desired address. Thus, there is a need for a system that reduces a fraudster's ability to effectively use stolen purchasing numbers by linking the purchasing number to a pre-stored delivery address that cannot be changed.

MY INVENTION SOLVES BOTH OF THESE PROBLEMS

21. My invention as set forth in the claims of the present application solves both of the above problems by (1) reducing the risk that a credit number might be stolen or compromised by creating a secure third party entity to hold consumer's credit cards and deliver only purchase authorizations and pre-stored delivery addresses to merchants when a purchase request is received, and (2) reducing the ability of a thief to use a stolen consumer identifier, such as a pin number, by limiting delivery of the purchased goods or services to only prestored delivery

addresses. Thus, even if a consumer's unique consumer identifier for making purchases through the claimed system is stolen, the consumer identifier can only be used to make purchases that will be delivered to the prestored delivery addresses, thereby eliminating the thief's ability to make purchases and have the goods delivered to the location of the thief's choice.

22. The claimed invention, therefore, removes a major loophole in present systems, i.e., the ability to ship to any location.

23. Moreover, as set forth in the claims of the present invention, the delivery address associated with a particular consumer identifier that has been compromised cannot be changed without disabling (e.g., rendering unusable) the consumer identifier that was compromised. This feature also frustrates the ability of thieves from using any acquired consumer identifiers.

24. Accordingly, the present invention as embodied in the claims comprises a system that combines a secure purchase processing system with the feature of permitting delivery of purchased goods to only pre-stored delivery address to thereby directly address the problem of online credit and debit card fraud and provides a solution thereto. The claimed system reduces the ability of thieves to both steal credit and debit card numbers and compromise alternative consumer identifiers by permitting delivery of purchased goods to only to prestored delivery addresses. Thus, I believe that my invention has a direct nexus to the long-felt need for a solution to the problem of fraudulent online credit and debit card purchases.

THE REFERENCES CITED BY THE EXAMINER DO NOT TEACH OR SUGGEST SUCH A SYSTEM

25. The references cited by the Examiner, namely the Lewis (U.S. Patent No. 6,233,565) and Egendorf (U.S. Patent No. 6,188,994) references, do not teach or suggest the claimed system.

26. Specifically, the Lewis reference does not teache a secure processing system that processes purchase requests without exposing payment information (e.g., credit/debit card numbers) to merchants and the feature of inextricably linking the consumer identifier to pre-

stored delivery addresses and rendering the consumer identifier inoperable in response to any change or attempted change to the delivery data as set forth in the claims as presently amended. Moreover, Lewis states that "after authentication is completed, the user then purchases the ultimate goods or services, postage in the case of the preferred embodiment, utilizing credit cards, ACH debit cards or checks as the method of payment, and electronically confirming the sale." Lewis, col. 3, lines 15-19. Thus, Lewis fails to teach or suggest a feature of the claims of the present application, namely the feature of using the payment data to pay for the purchased goods or services ***without exposing the payment data to the merchant***.

27. Similarly, the Egendorf does not teach or suggest a system that combines a secure purchase processing system with a consumer identifier that can be used to make purchases online and that is inextricably linked to pre-stored delivery addresses that cannot be changed without rendering the consumer identifier unusable. Further, Egendorf teaches specifying the means of delivery of the goods or services during the course of making a purchase. Thus, Egendorf fails to teach or suggest a feature of the claims of the present application, namely the feature of permitting delivery only to pre-stored delivery addresses.

28. Moreover, the Examiner fails to point to any motivation in either Lewis or Egendorf to suggest modifying those references to include the claimed features. The Examiner argues in the outstanding Office Action that the desire in Lewis to prevent fraud renders the claimed fraud prevention solution of combining secure purchase processing system that does not expose sensitive payment information with a consumer identifier inextricably linked to prestored delivery addresses such that to purchased good or services can only be delivered to the selected prestored delivery address. However, Lewis simply does not teach or even suggest these features and the Examiner's obviousness rejection amounts to a reconstruction of the Lewis reference in light of my disclosure. I am advised that such hindsight reconstruction is impermissible as a basis of a rejection.

29. Based on these differences between the cited references and the long-felt, but unresolved, need in the industry for a system that both (1) reduces the risk that a credit number might be stolen or compromised by creating a secure third party entity to hold consumer's credit cards and deliver only purchase authorizations and pre-stored delivery addresses to merchants when a purchase request is received and (2) reduces the ability of a thief to use a stolen consumer identifier, such as a pin number, by limiting delivery of the purchased goods or services to only pre-stored delivery addresses, I believe that my invention as embodied in the claims of the present application are non-obvious over the cited references and are therefore allowable.

30. I further declare that all statements made herein are of my own knowledge and are true and that all statements made on information and belief and believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Date: January 8, 2004

Andrew Casper